04-21-08

IFW AF

PTO/SB/21 (01-08)
Approved for use through 04/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 23

Application Number	10/642,256
Filing Date	08/15/2003
First Named Inventor	Wei Yuan
Art Unit	2134
Examiner Name	Tolentino, Roderick
Attorney Docket Number	P1028(16221RRUS02)

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Hemingway & Hansen, LLP		
Signature	D. Scott Hemingway		
Printed name	D. Scott Hemingway		
Date	April 18, 2008	Reg. No.	36,366

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Amy Kasper		
Typed or printed name	Amy Kasper	Date	April 18, 2008

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

P1028 (16221RRUS02) PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Yuan, Wei

Serial No.: 10/642,256

Filed: August 15, 2003

For: Method for Providing Media Communication Across Firewalls

Group Art Unit: 2134

Examiner: Tolentino, Roderick

Mail Stop Appeal Brief
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF FILED BY ASSIGNEE APPELLANT UNDER 37 C.F.R. § 1.192

The Assignee of Record, Nortel Networks Limited, hereby files this Appeal Brief pursuant to 37 C.F.R. §1.192, which appeals the basis of the claim rejections in the Final Office Action mailed on November 15, 2007 by the application Examiner. Appellant, Nortel Networks Limited filed a Notice of Appeal on February 15, 2007, which was received by the United States Patent and Trademark Office on February 19, 2007. Appellant believes the Examiner's final rejection is improper because the cited art relied upon by the Examiner fails

---

EXPRESS MAIL CERTIFICATE

"Express Mail" mailing label No. EM 015450743 US I hereby certify that this paper or fee is being deposited in triplicate with the United States Postal Service, "Express Mail" service under 37 C.F.R. 1.10, on the date indicated below and is addressed to Mail Stop Appeal Brief, P.O. Box 1450, Alexandria, VA 22313-1450.

April 18, 2008
Date of Deposit

Amy Kasper
Amy Kasper

04/22/2008 CCHAU1 00000009 10642256

01 FC:1402 510.00 OP

to disclose, teach or suggest critical claim limitations found explicitly in all the independent claims, and implicitly, in all the remaining claims of the patent.

For instance, the cited art relied upon for the Final Rejection fails to disclose, teach or suggest limitations found in the present invention such as the creation of a pinhole communication port in a firewall through the use of a trusted entity linked to the firewall, where the trusted entity is located outside the communication network. It is the trusted entity linked to the pinhole communication port and located outside the communication network, not an access router on the network, which supports the creation of a pinhole address and portal. The trusted entity receives information packets and forwards the information packets to that pinhole communication port address by replacing the packets header address information with the address of the pinhole communication port.

The independent claims, as well as the dependent claims, include numerous limitations that are not apparent from the art relied upon by the Examiner. This invention is not simple care-of addressing performed by an access router on the network after the packet has been transmitted through the firewall. The focus of the claimed invention is transmitting information packets to pinhole communication ports (with port addresses) in network firewalls by using a third party trusted entity provisioned outside the network to support two other devices communication on the network, and the replacement of the address header information before transmission to the pinhole communication port. It is believed the Examiner's rejection should be reversed, and the claims allowed because the claimed invention is not disclosed, taught or suggested in the cited prior art. For the foregoing reasons, the Examiner's Final Rejection should be reversed.

I. Real Party in Interest (37 C.F.R. §1.192(c)(1))

The real party in interest in this patent application examination is the Assignee of Record, Nortel Networks Limited, as reflected by assignment records at Reel/Frame 14401/0462.

II. Related Appeals and Interferences (37 C.F.R. §1.192(c)(2))

There are no other appeals or interferences relating to the present reexamination application.

III. Status of Claims (37 C.F.R. §1.192(c)(3))

Claims 1-20 are pending in this patent application, and each of those claims stand as finally rejected as noted in the Final Office Action mailed November 15, 2007.

1. Claims 1-13 and 15-18 were rejected under 35 U.S.C. § 103(a) as allegedly being anticipated by Trossen et al [20030212764] (hereafter "Trossen") in view of U.S. Patent 6,941,477 to O'Keefe (hereafter "O'Keefe").

2. Claims 14, 19 and 20 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Trossen in view of O'Keefe and in further view of Wu et al [2003021809] (hereafter "Wu").

IV. Status of Amendments (37 C.F.R. §1.192(c)(4))

No amendments have been filed or entered after the Final Office Action was mailed on November 15, 2007.

V. Summary of the Claimed Subject Matter (37 C.F.R. §1.192(c)(5))

A. The Problem Addressed By the Claims

Transmitting data information packets across a firewall presents difficulties, especially where the firewall cannot be specially configured to receive/not block signaling

messages sent from outside the firewall. Current methods for providing Voice over IP across firewalls and the present implementations of firewalls are ineffective in allowing the transmission of information packets across the firewall. The present invention provides a reasonable, and cost effective, solution to this problem.

B. The Solution Embodied in the Present Application

The present invention covers the creation of a pinhole communication port in a firewall through the use of a trusted entity linked to the firewall, where the trusted entity is located outside the communication network. The trusted entity receives information packets and forwards the information packets to that pinhole communication port address by replacing the packets header address information with the address of the pinhole communication port. It is the trusted entity linked to the pinhole communication port and located outside the communication network, not an access router inside the network, which replaces the header information and provides the functionality to get the firewall to allow the information packet to be transmitted through it.

The independent claims, as well as the dependent claims, include numerous limitations that are not apparent from the art relied upon by the Examiner. This invention is not simple care-of addressing performed by an access router after the packet is transmitted through the firewall. The focus of the claimed invention is transmitting information packets to pinhole communication ports (with port addresses) in network firewalls from outside the firewall and outside the network by using a third party trusted entity provisioned outside the network to support two other devices communication on the network. The trusted entity located outside the network supports the replacement of the address header information

before transmission to the pinhole communication port. It is believed the Examiner's rejection should be reversed, and the claims allowed.

VI. Issues (37 C.F.R. §1.192(c)(6))

The sole issue is whether the cited prior discloses, teaches or suggests the claimed subject matter in the manner set forth by the Examiner in the 35 U.S.C. §103 rejection.

VII. Groupings of the Claims (37 C.F.R. §1.192(c)(7))

Because all the Examiner's rejection of each claim relies in whole or in part on the Trossen and O'Keefe references, all Claims 1-20 can be grouped into Group 1. Independent Claims all include explicit limitations that are not disclosed, taught or suggested by the cited art. These independent claims stand or fall together, and as such, all the claims 1-20 stand or fall based on the Board's analysis of the cited art references.

VIII. Argument (37 C.F.R. §1.192(c)(8))

A. Summary of the Rejection

Trossen provides for one content source providing media content to handoff to a second content source when a mobile terminal moves from one domain to another. Trossen is the sole cited reference relied upon by the Examiner that addresses the creation of a pinhole, but these actions are not done by a trusted entity located outside the network (as claimed in the present invention). Trossen and the other cited reference fail to disclose essential claim elements alone or in combination of the claimed invention.

The Examiner relies on the following paragraph from Trossen to support his rejection, which read as follows:

> [0007] The present invention provides for a relocation of content sources that provide media content to a mobile terminal (mobile node) when a network layer-level handoff occurs. The relocation of content sources enables the mobile terminal to seamlessly execute an application that utilizes the media

> content from a current content source before the handoff and from a new content source after the handoff. The mobile terminal registers with a current access router in order to inform the access router about application context information. The current access router informs a new access router about the impending handoff. The new access router consequently discovers the new content source.

This paragraph discusses the hand-off event, but there is nothing in Paragraph 7 of Trossen which discloses, teaches or suggests the use of an external trusted entity located outside the communication network (but linked to the firewall) to communicate information packets through the firewall in the destination network. There is nothing in this paragraph that discloses, teaches or suggests the use of an external trusted entity (outside to the destination network, but linked to its firewall) to replace headers and create a pinhole in the firewall for a communication.

The Examiner also relies on the following paragraph from Trossen to support his rejection, which read as follows:

> [0008] In an embodiment of the invention, the network comprises a current access router, a current content source, a new access router, and a new content source. The new access router and the new content source may be associated with a different administrative network domain than the current access router and the current content source. The embodiment supports an Internet protocol (IP) as the network layer, although other embodiments can support other network layer protocols (corresponding to the third layer of the Open Systems Interconnection model). Before an IP-level handoff, the current access router and the current content source provides media content to the mobile terminal. The mobile terminal registers with the current access router in order to provide application context information that is associated with the application. The current access router informs a new access router in response to an impending handoff. The new access router consequently discovers the new content source, which is able to provide the media content for the application. The new content source consequently establishes an IP path to the new care-of address of mobile terminal, via new access router. When the IP-level handoff does occur, the current content source informs the new content source about the current state of the application in order that the new content source can resume the application in a seamless manner.

This paragraph discusses the hand-off procedures, but there is nothing in Paragraph 8 of Trossen which discloses, teaches or suggests the use of an external trusted entity located outside the communication network (but linked to the firewall) to communicate information packets through the firewall in the destination network. There is nothing in this paragraph that discloses, teaches or suggests the use of an external trusted entity (outside to the destination network, but linked to its firewall) to replace headers and create a pinhole in the firewall for a communication.

The Examiner also relies on the following paragraph from Trossen to support his rejection, which read as follows:

> [0024] With a state creation procedure 217, new content source 119 configures the new IP path between new content source 119 and new access router 117 (corresponding to the new care-of address) according to states (e.g. QoS level) that are consistent with the media description. QoS establishment along the new path can be done using protocols such as Resource Reservation Protocol (RSVP), or other QoS signaling protocols that are being designed in the Next Steps in Signaling (NSIS) working group of IETF. Configuring the new IP path may also involve creating a pinhole in the firewall that may reside between the new access router 117 and the new content source 119. The new IP path may not be able to support the media description that is supported by the current IP path (current content source 111 to network 113 to current access router 109 to base transceiver station 107). In such a case, new content source 119 may redefine the media description (e.g. modifying the coding format, altering resolution, resizing, and adjusting the degree of motion) and send the modified media description to the new care-of address of mobile terminal via the new access router 117 as part of state creation procedure 217. The communication of new media description may be done using SIP messages. In the embodiment, new access router 117 stores the modified media description (or the corresponding SIP message). New access router 117 subsequently sends the modified media description (or the corresponding SIP message) to mobile terminal 105 in an action 223 when mobile terminal 105 performs the IP-level handoff. In another embodiment, the new access router can send the modified media description (or the corresponding SIP message) to mobile terminal 105 via the current access router 109. Mobile terminal 105 acknowledges the reception of the modified description with a confirmation message 225.

This paragraph is the only mention of a pinhole. This mention (only in one sentence) in Paragraph 24 of Trossen fails to disclose, teach or suggest the use of an external trusted entity located outside the communication network (but linked to the firewall) to communicate information packets through the firewall in the destination network. There is nothing in this paragraph that discloses, teaches or suggests the use of an external trusted entity (outside to the destination network, but linked to its firewall) to replace headers and create a pinhole in the firewall for a communication.

The content source in Trossen originates the media content being transmitted and does not disclose any of the external trusted entity functionality as claimed. This router function is not disclosed, taught, or suggested in Paragraph 007 or 0024 of Trossen or by the "trusted content server" of O'Keefe. Trossen does not disclose the creation of a pinhole request or creating a pinhole communication port in the firewall in response to the creation of a pinhole request. Trossen fails to disclose any mechanism for creating a communication pinhole port, including the use of a trusted entity, use of create pinhole request, use of create pinhole response, or updating a routing table with the address designation of a communication pinhole port.

Trossen only states that "[c]onfiguring the new IP path may also involve creating a pinhole in the firewall that may reside between the new access router 117 and the new content source 119." *Trossen, paragraph 0024.* This statement, however, never discloses, teaches, or suggests any mechanism for creating the pinhole by an external trusted entity that is outside the destination network and linked to its firewall. Furthermore, there is nothing stated in the RSVP or SIP protocol that teaches, suggests, or discloses a specific create pinhole message request or create pinhole message response or any possible role in creating

pinholes through firewalls. *See File History, RFC: 2205 "Resource Reservation Protocol", Braden, September 1997.*

Concluding that the content source functions in any analogous manner as the trusted entity, requires the Examiner to make impermissible, unsupported assumptions regarding the pinhole creation. *See In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 177 (CCPA 1967), cert. denied, 389 U.S. 1057 (1968). It is respectfully submitted that the Examiner's rejections uses the claimed invention as a guide to impermissibly read into the reference (through hindsight reconstruction) unsupported assumptions on how the IP path is configured, pinholes created, and packets transmitted. *See In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 177 (CCPA 1967), cert. denied, 389 U.S. 1057 (1968).

The Examiner appears to believe that numerous claim elements are inherent to various basic teachings of Trossen. However, Trossen does not describe any mechanism or procedure that creates a pinhole or transmits a packet through a firewall. Essential claim elements in the independent claims (but not shown in Trossen) include the trusted entity replacing an address in the address header of an information packet with an address for the communication pinhole so the information packet can be transmitted through the pinhole to the communication device.

Also, O'Keefe is cited as support for a trusted entity (i.e. O'Keefe's trusted content server), which the Examiner admits is not taught in Trossen. However, the trusted content server in O'Keefe does not perform any router functions or have any role in creating pinholes in a firewall. O'Keefe does not teach, suggest, or disclose a trusted entity as claimed, because it fails to function as claimed. It apparently functions to create and transmit information packets derived from documents collected from databases and verified by a

separate verification server and does not make any address substitutions (i.e. it is the source of the IP packets).

The independent claims in the present invention are simply not taught by the cited references, which rely upon Trossen to disclose the routing functionality by the trusted entity. There is no suggestion within the references that the content sources in Trossen have any role in creating pinholes, and none of the cited references teach, disclose, or suggest any procedure or exchanged messages for creating a pinhole. O'Keefe also fails to disclose any of the claimed routing functionality or a trusted entity as claimed, so the two references cannot sustain a § 103 rejection.

B. The Examiner's Reliance on Trossen and O'Keefe is Misplaced With Respect to Claims 1, 8, and 15

The Examiner relies on Trossen as the primary reference to support his invalidity rejection under 35 U.S.C. §103(a). As shown in Figure 2 of Trossen, the Trossen reference discloses an IP-level hand-off procedure where a Mobile Terminal (105) is initially connected to a first Content Source (111) through current Access Router (109). The Mobile Terminal (105) is handed off to a new Access Router (117) and new Content Source (119), after some initial preliminary communications between these devices.

1. The Disclosure of a Pinhole in a Firewall is Not Enough To Invalidate the Claimed Invention

Trossen only states that "[c]onfiguring the new IP path may also involve creating a pinhole in the firewall that may reside between the new access router 117 and the new content source 119." *Trossen, paragraph 0024*. This statement, by itself, never discloses, teaches, or suggests any mechanism for creating the pinhole communication port, linking that pinhole communication port to a trusted entity outside the network, or using that

communication port as a forwarding address by such a third party trusted entity. Trossen fails to disclose the use of a trusted entity, use of create pinhole request, use of create pinhole response, or updating a routing table with the address designation of a communication pinhole port.

The access router in Trossen inside the network does not perform the claimed invention by simple care-of addressing after receiving an information packet through the firewall. That is not the same thing as the claimed invention, and such a conclusion appears to have been based on impermissible hindsight reconstruction and modification of the prior art using the claimed invention as a roadmap. *See In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 177 (CCPA 1967), *cert. denied*, 389 U.S. 1057 (1968). Trossen simply does not support the Examiner's rejection.

The Examiner's Final Office Action Rejection admits that there is no teaching in any cited reference as to how the pinhole is created in Trossen, or that such creation is similar to the manner in which the claimed invention requires that creation of a pinhole communication port. The Examiner states "[t]here has to be some form of messaging that goes on in order to create the pinhole," but he does not indicate what that messaging would be. *Final Rejection, ¶3, p. 2.* Even if some form of messaging were required, there is no indication in the cited references (or anywhere else) that the messaging and use of the trusted entity as claimed in the present invention is disclosed, taught or suggested in Trossen or any other cited reference.

The Examiner claims that such teachings are shown in the RSVP protocol (RFC 2205), which can be combined with the teachings of Trossen. *Final Office Action, ¶14, p. 6.* The RSVP protocol (RFC 2205), however, does not address pinholes or firewalls. The words "pinhole" and "firewall" do not even appear in that RFC 2205 for the RSVP Protocol. As

such, the RSVP protocol does not disclose, teach or suggest the claimed invention when combined with Trossen. Overall, nothing in Trossen or the RSVP protocol discloses, teaches or suggests the claimed invention.

2. No Disclosure in Trossen or O'Keefe of a Trusted Entity Creating A Pinhole in a Firewall

There is nothing in Trossen that suggests that a third party trusted entity would perform address header replacement to forward packets to the pinhole communication port address before transmission through the firewall. Nothing in Trossen discloses a separate "trusted entity" or even suggested that a separate device connected to a firewall and located outside the communication network could be used in conjunction with the Trossen IP hand-off procedure.

The Examiner relies on O'Keefe to teach a "trusted content server," but the trusted entity in O'Keefe is not used in conjunction with a pinhole communication port. The trusted content server in O'Keefe does not perform any router functions or have any role in creating pinholes in a firewall. In fact, the words "pinhole" and "pinhole communication port" are not used anywhere in the O'Keefe reference. Simply replacing the trusted content server in O'Keefe with the content server in Trossen would still not result in the trusted entity claimed in the present application. Nothing in Trossen or O'Keefe discloses, suggests or teaches the claimed invention.

c. Simple Care-of Addressing in Trossen is Not the Claimed Invention

The Examiner claims that the care-of addressing performed by the access routers is the same as the address header replacement performed by the trusted entity in the claimed invention. *Final Office Action, ¶4, p. 3.* Trossen, however, performs simple care-of addressing after the information packet has been transmitted through the firewall, and the

care-of addressing in Trossen has nothing to do with the creation of the pinhole communication port by a trusted entity or the transmission of the information packet to that pinhole communication port address as claimed.

The claimed invention, on the other hand, is using address header replacement before transmission of the information packet to the pinhole communication port and is essential to getting the information pack to that pinhole communication port. This is a fundamental difference between the teachings in Trossen and the claimed invention. Nothing in Trossen discloses, teaches or suggests the claimed invention.

IX. Conclusion

The Applicant respectfully requests reversal of the claim rejections in the examination in light of the remarks. This appeal brief is filed with a fee of $510.00. It is believed that no additional fees are necessary for this filing. If additional fees are required for filing this response, then the appropriate fees should be deducted from D. Scott Hemingway's Deposit Account No. 501,270.

Respectfully submitted,

D. Scott Hemingway

D. Scott Hemingway
Reg. No. 36,366
Attorney for Applicant and
Assignee of Record

Hemingway & Hansen, LLP
1717 Main Street
Comerica Bank Tower – Suite 2500
Dallas, Texas 75201
(214)292-8301 (voice)
(214)739-5209 (fax)

Date: 4/18/08

VIII. Appendix (37 C.F.R. §1.192(c)(9))

Appendix of Claims

APPENDIX OF CLAIMS:

1. (Original) A packet-based communication network for communication through a communication network gateway comprising:

a firewall on the communication network gateway for securing communications to and from the network;

a communication device on the communication network connected to the firewall by a communication link;

a trusted entity linked to the firewall by a communication link, said link allowing information packets to be sent to a first communication pinhole through the firewall to the communication device; and

said trusted entity replacing an address designation in the address header of one of said information packets with an address designation for the first communication pinhole so the information packet can be transmitted through said pinhole to said communication device.

2. (Original) The packet-based communication network for communication through a communication network gateway of Claim 1 wherein the first communication pinhole is established using signaling messages transmitted through the firewall.

3. (Original) The packet-based communication network for communication through a communication network gateway of Claim 2 wherein the signaling messages include a create pinhole message.

4. (Original) The packet-based communication network for communication through a communication network gateway of Claim 2 wherein the signaling messages include a create pinhole acknowledge message.

5. (Original) The packet-based communication network for communication through a communication network gateway of Claim 1 wherein the trusted entity is a media proxy router.

6. (Original) The packet-based communication network for communication through a communication network gateway of Claim 1 wherein the trusted entity includes a component with a soft-ware functional switch.

7. (Original) The packet-based communication network for communication through a communication network gateway of Claim 1 wherein the communication network includes an application server on the communication link between the firewall and the communication device.

8. (Original) A method for routing information packets across a firewall to a packet-based communication network comprising the steps of:

receiving a create pinhole request at a trusted entity linked to the firewall of the communication network and located outside the communication network;

creating a pinhole communication port in the firewall in response to the create pinhole request;

receiving a first information packet at the trusted entity to be transmitted across the firewall through said pinhole;

replacing an address in the information packet address header information with a communication port address for a pinhole created in the firewall; and

forwarding the information packet to a destination address across the firewall using the communication port address for the pinhole communication port.

9. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 further comprising the steps of:

creating a communication port address routing table association on the trusted entity for designated pinhole ports in the firewall using address data from the create pinhole request.

10. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 further comprising the steps of:

transmitting said create pinhole request from the end-terminal to the trusted entity; and

receiving a create media pinhole acknowledgement at the end-terminal containing the communication port address.

11. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 further comprising the steps of:

transmitting said create pinhole request from an application server to the trusted entity; and

receiving a create media pinhole acknowledgement at the application server.

12. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 wherein the application server is a session initiation protocol proxy server.

13. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 wherein the application server is an integrated access device.

14. (Original) The method for routing information packets across a firewall to a packet-based communication network of Claim 8 wherein the application server is an application proxy server.

15. (Original) A method for using a pinhole communication port in a packet-based communication network firewall comprising the steps of:

providing a trusted entity having an input and an output outside the communication network;

linking said trusted entity to the pinhole communication port;

transmitting a first signal from the communication network to the input of the trusted entity, wherein said signal has an address designation for said pinhole communication port;

providing a routing table on the trusted entity with the address designations for the pinhole communication port;

receiving a packet transmission at the input of the trusted entity to be sent to a communication device inside the communication network;

placing the address designation for the pinhole communication port as the address header of the packet transmission; and

transmitting the packet transmission from the output of the trusted entity to the pinhole communication port for transmission onto the communication device.

16. (Original) The method for using a pinhole communication port in a packet-based communication network firewall of Claim 15 further comprising the step of:

transmitting a second signal from the output of the trusted entity containing the address designation of the communication port, wherein said second signal acknowledges receipt of the first signal.

17. (Original) The method for using a pinhole communication port in a packet-based communication network firewall of Claim 16 further comprising the step of:

receiving the second signal at the communication device.

18. (Original) The method for using a pinhole communication port in a packet-based communication network firewall of Claim 16 further comprising the step of:

receiving the second signal at a server on the communication network.

19. (Original) The method for using a pinhole communication port in a packet-based communication network firewall of Claim 15 wherein the transmission packet contains voice data.

20. (Original) The method for using a pinhole communication port in a packet-based communication network firewall of Claim 15 wherein the transmission packet is a real time transport protocol information packet.